# Review of the Contraband Phone Task Force Status Report

June 19, 2019

This document is provided to the House and Senate Appropriations Subcommittees on Financial Services and General Government to formally comply with an informational briefing directive in the Fiscal Year 2019 Omnibus Explanatory Statement.[1] That language specifically directed the Federal Communications Commission (FCC or Commission) to brief the Committees on Appropriations on a timeline for further addressing the contraband cell phone in prisons issue and to provide the status of any reports the FCC received from the Contraband Phone Task Force. The Explanatory Statement further directed the FCC to share with the Committees any barriers that arise and prevent the FCC from meeting the specified timeline. FCC staff discussed this Report with representatives of the Federal Bureau of Prisons (BOP) and the National Telecommunications and Information Administration.

The FCC staff consulted with the Appropriations Committee staff concerning the outstanding Contraband Phone Task Force Report within 60 days of passage of the 2019 Omnibus. The Commission's staff continued to report to Committee staff on the Report's status, and ultimately notified the Committee staff of the April 26, 2019 Report filing.

Accordingly, this review of the Contraband Phone Task Force Status Report highlights recent industry developments related to the important public safety issue of preventing contraband cell phone use in our nation's correctional facilities. The Task Force, comprised of the Cellular Telecommunications Industry Association (CTIA), the Association of State Correctional Administrators, the Federal Bureau of Prisons, various wireless providers, and state corrections officials from various individual states, has been examining the technological, legal, and administrative challenges and solutions to combat this serious problem.[2] In addition to discussing the Task Force Report, which is appended hereto,[3] our review includes an update on ongoing Commission efforts in this area.

---

[1] *See* S. Rep. No. 115-281, at 68 (2018); *see also* Consolidated Appropriations Act, 2019, Pub. L. No. 116-6, Explanatory Statement (H. Rept. 116-9, Division D, Title V, p. 673), 133 Stat. 13 (2019) (stating "Unless otherwise noted, the language set forth in . . . Senate Report 115-281 carries the same weight as language included in this joint explanatory statement and should be complied with unless specifically addressed to the contrary in this joint explanatory statement.").

[2] As noted in the Contraband Phone Task Force Report (Task Force Report or Report), the participating wireless providers are AT&T, Sprint, T-Mobile, and Verizon, and the participating state departments of corrections are: Alabama, Arkansas, California, Indiana, Mississippi, Oklahoma, South Carolina, Tennessee, and Texas. Although the BOP is an ex officio member of the Task Force, it does not endorse the final Report as submitted by CTIA and ASCA.

[3] The appended Report is a redacted version, as CTIA and ASCA sought confidentiality of certain sensitive matters in the Report.

*Task Force Report: Establishment of Contraband Interdiction Systems Testbed, Managed Access Systems Testing Results and Recommendations*. In the Task Force Report, CTIA and ASCA summarize the Task Force's activities since its April 2018 inception, including the collaboration among stakeholders, the results of the Contraband Interdiction System (CIS) Testbed – established for the technical assessment of CIS technologies – which provide insight into two managed access technologies (a type of CIS that captures and drops calls from prison inmates), and recommendations for best practices for CIS deployments that provide a roadmap for future improvement. As detailed in the Task Force Report, at the first Task Force meeting in April 2018, the group agreed upon the scope and manner of testing CIS technologies and retained the Virginia Tech Applied Research Corporation and Dr. Charles Clancy to lead the team. The testing and evaluation occurred between April 2018 and January 2019, both in the field at two correctional facilities in South Carolina and Texas, and in laboratory conditions. The Testbed included two managed access systems (MAS) that proved to be generally successful in interdicting communications from contraband devices in most areas of the correctional facilities. In addition, the testing confirmed that signals from both MAS solutions were generally contained within the correctional facilities, suggesting that the systems posed little risk of interference to legitimate wireless users outside the facilities' perimeters. Overall, the testing confirmed the effectiveness of managed access technology and its potential utility for helping combat contraband device use, provided there is ongoing maintenance and monitoring of the interdiction systems. Ideally, ongoing maintenance includes the detection of changes in surrounding cellular networks, so that appropriate MAS adjustments can be made to maintain effectiveness, reports of any destruction of MAS equipment by inmates, and any other issues that could impact MAS operations.

Based on the testing and analysis, the Task Force Report provides several recommended guidelines and best practices for the operation of CIS systems, including technical, administrative, and physical security considerations for solutions providers, wireless providers, and corrections officials. Significant among these MAS best practices is the idea of continual radio frequency (RF) testing and monitoring as well as communication between correctional facility officials, MAS vendors, and wireless providers. We anticipate that these best practices will provide a roadmap for improvement and that the Task Force will continue to refine the recommendations for MAS solutions to be more effective and affordable.

*Use of Stolen Phone Database and State Court Order Processes*. One issue discussed in both the record of the Commission's contraband proceeding and the Task Force Report is the use of radio-based monitoring technologies to obtain contraband phone identifying information in connection with state-level court orders to require the permanent disabling of identified contraband wireless devices. The Task Force reports that correctional authorities in approximately six states[4] are implementing this tool to combat contraband phone use. As part of its commitment when establishing the Task Force, CTIA has facilitated the use of the wireless industry's existing Stolen Phone Database (SPD) as a complement to the court order process. By entering into the SPD the disabled phone's identifying information, it is prevented from being reactivated on another wireless carrier's network. CTIA plans to work with the SPD administrator to establish a contraband device designation in the SPD to enable enhanced

[4] The six states include California, South Carolina, Georgia, Mississippi, Tennessee, and Indiana.

reporting and recordkeeping on listed contraband devices. We note that CTIA has identified the challenge of the scalability of the court order process, as law enforcement rules and procedures vary from state to state.

*MAS Evolved*. The Task Force Report identifies additional significant challenges to solving the contraband wireless device problem. The evolution of wireless device technology from 2G to widespread 4G and 5G deployments presents the need for continued upgrades to maintain long-term MAS effectiveness. Not only will wireless providers' deployments of 5G require MAS solutions providers to deploy additional frequency bands, but network security issues must be overcome to be effective against 4G/5G phones, given the wireless providers' ultimate phase-out of current 2G network technologies. In addition, corrections officials may have difficulty communicating with each other within certain areas of a correctional facility, for example in locations with weaker coverage or in between MAS coverage zones. The Report includes recommended next steps for dealing with these challenges and exploring ways to more efficiently engage 4G and 5G technologies. We strongly encourage the Task Force to implement what is described in the Task Force Report as "MAS Evolved," which envisions a partnership between MAS vendors and wireless providers via roaming agreements for network security reasons. The Report suggests that a lower cost MAS solution may be possible based on the use of small cells and recommends testing. We will certainly provide assistance to the Task Force as needed on this approach.

*Geofencing*. The Task Force Report also discusses the concept of geofencing which, in the contraband context, refers to wireless providers using their network to determine whether a particular mobile device is located within the geographic boundary of a correctional facility and then restricting cellular services if that device is not authorized to operate in that area. CTIA has identified various challenges to implementing a geofencing solution, including both technical and legal (such as privacy concerns) that must be overcome for successful deployment. We support Task Force efforts to explore whether geofencing can develop into a feasible, legal, and cost-effective solution.

*Jamming*. As to the feasibility of jamming technology, the Testbed included one jamming solution tested in a laboratory setting. In the Task Force Report, CTIA calls for the BOP to conduct field tests and provides a technical map for future testing of jamming solutions. The Task Force did not conduct jamming field tests because of the current legal framework prohibiting the use of jammers by state and local correctional facilities. While not prohibited in federal facilities, we are not aware of any permanent federal deployments of jamming solutions. However, the Task Force Report references jamming tests conducted by NTIA and the BOP in a federal prison in Cumberland, Maryland in January 2018,[5] and most recently in April 2019 at Broad River Correctional Institution, a state prison located in Columbia, South Carolina. The Broad River test was made possible through the "deputization" of state and local officials resulting from substantial federal direction and supervision and use of federally owned or controlled jamming equipment. An NTIA report analyzing the data collected from the Broad

[5] As noted in the NTIA report released in June 2018 following the Cumberland, Maryland jamming test, the jammer tested was designed to prevent cellular communications within a single correctional facility cell. In this regard, the test was limited, and the report does not address the potential for interference to wireless services outside of the single correctional facility cell.

River jamming test is forthcoming. We agree with the Task Force Report's conclusion that additional field testing of jamming technology will provide a better understanding of the challenges and costs associated with the proper deployment of jamming systems, and we support the expansion of testing to include deployments in non-federal facilities through the deputization model. Regarding deployment costs, we note that any active radio-based technology used to combat contraband cellphones must bear the cost of careful engineering, installation, and system maintenance to avoid causing interference to lawful radio communications inside or outside the correctional facility.

*Commission Action to Streamline CIS Deployment and Promote Collaboration.* Because there is no one-size-fits-all solution to this problem, the Commission has facilitated the use of various radio-based technical solutions and is considering how other approaches may help. In early 2017, after engaging with a wide array of stakeholders, the Commission adopted rules to allow for immediate review and approval of CIS. The Commission's revised rules seek to facilitate prompt transactions between wireless providers and solutions providers (on behalf of departments of correction). Currently, FCC-authorized CIS systems are deployed at approximately 65 correctional facilities in ten states. As part of the Commission's proceeding, we also sought to develop a record through industry participation on the viability of new technologies to address the contraband issue. The FCC continues to meet with solutions providers, wireless providers, and state department of corrections officials, and provide guidance with spectrum leasing activities to support industry efforts to deploy lawful, cost effective solutions.

To facilitate discussions among stakeholders regarding progress, updates on technical solutions, and continuing challenges, Chairman Pai held a successful fact-finding meeting on February 7, 2018 that included state corrections officials, solutions providers, public safety experts, wireless providers, Department of Justice officials, and BOP representatives. Participants discussed their challenges and requirements for combatting this public safety issue, including funding issues and deployment strategies, and possible alternative strategies and methods. Importantly, representatives from the wireless industry agreed to work closely with the corrections community and solutions providers and establish a task force to further consider the best methods of developing and deploying cost-effective technologies to solve this difficult problem. The FCC is encouraged that since CTIA launched the Task Force with ASCA a few months after the meeting, a wide range of stakeholders are developing relationships and continuing to examine methods of refining current technical solutions, as well as exploring the viability of new solutions to this problem.

The Commission intends to continue to work with members of the Task Force and other stakeholders in the coming months on any issues that require the FCC's expertise. The Commission is committed to facilitating the development and widespread deployment of lawful technological solutions that combat contraband device use while protecting legitimate communications.